УДК 343.9

Д. С. Захаров,
курсант 2-го курса факультета милиции
Могилевского института МВД
Научный руководитель: Д. И. Шнейдерова,
преподаватель кафедры уголовного процесса
и криминалистики Могилевского института МВД

АКТИВНЫЕ МЕРЫ ПРОФИЛАКТИКИ И ПРЕДУПРЕЖДЕНИЯ ХИЩЕНИЙ В СЕТИ ИНТЕРНЕТ

Всемирная глобальная сеть Интернет не только предоставляет безграничные возможности коммуникации и взаимодействия добросовестным пользователям, но и привлекает субъектов преступной активности возможностью внедрения своего противоправного потенциала в сферу информационных технологий. Согласно статистическим данным Министерства внутренних дел Республики Беларусь, по итогам 2019 года был установлен стремительный рост количества совершаемых на территории Республики Беларусь киберпреступлений. Так, в 2019 году было зарегистрировано 10 539 (+5 798) преступных фактов, что в 2,2 раза больше, чем в 2018 году [1]. При этом следует отметить, что большую часть всех киберпреступлений составляют хищения, совершенные с использованием возможностей современных технических устройств и сети Интернет. Среди преобладающих составов выделяются мошенничество, вымогательство и хищение путем использования компьютерной техники, сопряженное с несанкционированным доступом к компьютерной информации.

Мошенничество характеризуется как наличием примитивных форм обмана, так и более профессионально продуманных. К примитивному мошенничеству можно отнести сделки купли-продажи, осуществляемые посредством двустороннего контакта между продавцом и покупателем через сервисы обмена и продажи различных товаров и услуг, социальные сети и мессенджеры, а также просьбы о переводе средств на предоставленный счет от лица знакомых и друзей, попавших в беду, получаемые потерпевшими посредством сообщений в социальных сетях. Профессиональное мошенничество в сети Интернет требует от преступников наличия знаний веб-программирования либо привлечения к соучастию лиц, ими обладающих. Злоумышленниками создаются «сайты-однодневки» или «сайты-близнецы» реальных интернет-сервисов с возможностью покупки соответствующих товаров и услуг либо перевода средств. Распространенными примерами являются сервисы с онлайн-играми, где участнику необходимо приобретать героев, инвентарь или их определенные способности, ключи к

новым уровням, либо рекламные сайты о розыгрыше или продаже за половину стоимости популярных гаджетов и другие.

Кибервымогательство связано с распространением в сети Интернет вирусного программного обеспечения, способного блокировать доступ к данным, хранящимся в памяти любого устройства, принадлежащего как физическим лицам, так и крупным организациям. Распространение вирусные программы получают благодаря посещению пользователями непроверенных сайтов, скачиванию или запуску подозрительных файлов и приложений, открытию получаемых по электронной почте от незнакомых лиц ссылок, активирующих загрузку и установку вируса. За ключ доступа к поврежденным данным вымогатели требуют определенную сумму, как правило, в криптовалюте, анонимность и децентрализация которой позволяет им оставаться неуязвимыми перед правоохранительными органами [2, с. 303].

Хищения путем использования компьютерной техники по своему количеству занимают лидирующую позицию в системе всех хищений, совершаемых посредством глобальной сети. Развитие возможностей компьютерного программирования привело к появлению таких высокотехнологичных способов осуществления несанкционированного доступа к личным данным пользователей, как фишинг, фарминг, сим-свопинг, смишинг и другие.

Первоочередной причиной успеха киберпреступников является компьютерная и сетевая безграмотность пользователей, преодоление которой возможно благодаря проведению правоохранительными органами профилактической работы в данном направлении. Несмотря на успешно реализуемые пассивные меры профилактики, к которым можно отнести ведение информационных стендов, размещение информации на официальных сайтах органов внутренних дел, назрела необходимость во внедрении активных мер. Активная деятельность должна базироваться на непосредственном контакте сотрудников правоохранительных органов с населением посредством участия в информационных акциях, проводимых в рамках дней информирования с работниками организаций и учащимися образовательных учреждений. Эффективным видится метод организации ежеквартальных горячих линий в эфирах национальных каналов теле- и радиовещаний, где сотрудники могли бы не только доводить до сведения населения необходимую информацию, но и в режиме реального времени отвечать на возникающие у пользователей вопросы. Еще одной активной формой деятельности по предупреждению киберпреступлений может стать взаимодействие правоохранительных органов с интернет-провайдерами. Данная мера представляется в виде налаженного двустороннего контакта провайдеров с подразделениями по раскрытию преступлений в сфере высоких технологий, в рамках которого воз-

можен обмен данными о наличии активности вызывающих подозрение пользователей, онлайн-сервисов, интернет-магазинов и других субъектов интернет-пространства, а также принудительная блокировка доступа к их услугам.

1. Профилактика киберпреступлений [Электронный ресурс] // Официальный сайт УВД Могилевского облисполкома. URL: https://mogilev.mvd.gov.by/ru/news/2566 (дата обращения: 20.05.2020). Вернуться к статье

2. Шнейдерова Д. И. Криминалистическая характеристика криптовалюты как средства и предмета преступного посягательства // Актуальные проблемы учения о преступлении : тез. докл. и сообщ. междунар. науч. конф., посвящ. 90-летию со дня рождения А. И. Марцева, Омск, 28 февр. 2020 г. / Омская академия МВД России ; ред.: В. В. Бабурин [и др.]. Омск, 2020. С. 300–305. Вернуться к статье